Title: Homomorphic Encryption Scheme Parties, Platforms, Techniques, Complexities, Limitations and Future Directions: A Systematic Review

Joshua Mamza[1], I. Ismaila[2], J. A Ojeniyi[3], S.M Abdulhamid[4], M.D Noel[5] and S. Ahmad[6]
[1,2,3,5,6]Cyber Security Science Department, Federal University of Technology Minna, Niger State, Nigeria
[4]Information Technology Department, Community College of Qatar

Joshua.pg6759@st.futminna.edu.ng

Ismi.idris@futminna.edu.ng

ojeniyija@futminna.edu.ng

shafii.abdulhamid@ccq.edu.qa

moses.noel@futminna.edu.ng

ahmads@futminna.edu.ng

Abstract
Homomorphic Encryption (HE) is a cryptographic encryption technique that allows computational functions being carried out on encrypted data with the view of maintaining the functional properties of the data that is encrypted. The outcome is that the computation performed on the encrypted data remain the same as the decrypted data. Homomorphic Encryption revolved around privacy enhancing technology which react to the challenges of data sharing in an organization such as Personal Identifiable Information, Health Care Information, and Financial Transaction Data. All these data require privacy which is a prevalent issue. Significant achievement and advancement has been achieved in the design, development and implementation of HE techniques, thereby enhancing their efficiency and its practical applicability. This study would explore the parties, platforms, techniques, complexities and limitations associated with HE Schemes. Articles written in English, published in peer-reviewed academic journals, and released between 2020 and 2025 met the inclusion criteria. In the end, this study examined 40 relevant articles in total. The review delves into the most recent advancement in HE techniques, complexities and limitations. Also, focus is given to the roles and responsibilities of various stakeholders, platforms and challenges encountered in real world application. Our key finding indicates that while HE offers important privacy benefits on applications, its deployment may be hindered by massive computational and communication overheads. This study clarifies the potential of HE in addressing the challenges in data privacy and security as it is applied in real-world situations such as cloud computing environments and federated learning while maintaining its computation feasibility.

Key words: Homomorphic Encryption, Fully Homomorphic Encryption, Privacy-Preserving computations, Multi-Party Computations and Platform

SECTION I

INTRODUCTION

The word “homomorphic” originates from abstracts algebra. Homomorphism in algebra means the property that’s maps the connection that exist between two algebraic assemblies which does not easily (Wu et al., 2025). This idea has been protracted to cryptographic scheme which has become an encryption technique that allows computational functions being carried out on encrypted data, there for maintaining the functional properties of the data that is encrypted, thereby allowing the outcome of the computation performed on the encrypted data to remain the same as the decrypted data (Wu et al., 2025)(Shah and Sivakumar 2026). HE evolves around privacy enhancing technology which react to the challenges of data sharing in an organization such as Personal Identifiable Information, Health Care Information, and Financial Transaction Data etc. All these data are requiring privacy which is a prevalent issue (Mohan Das Viswam, 2022).The concept of HE has been established for decades; however, the first Fully Homomorphic Encryption scheme (FHE) was introduced by Craig Gentry in the year 2009 (Ahn *et al.*, 2025). Ever since, the significant achievement and advancement has been achieved in the design, development and implementation of HE techniques, thereby enhancing their efficiency and its practical applicability (Ahn *et al.*, 2025). The systematic literature review aims to provide a comprehensive over of HE techniques, focusing on recent developments and implementations. HE will explore the parties, platforms, techniques, complexities and limitations associated with HE Scheme. This review is built upon surveys and systematic reviews that are existing (Yousuf *et al.*, 2021) by integrating research from 2020 to 2025. The review aims to provide the research space with clear understanding of HE Schemes and their potential to addresses the existing and the new challenges of data privacy and security.

Table 1: Abbreviations Table

Abbreviation	Meaning
SLR	Systematic Literature Review
HE	Homomorphic Encryption
FHE	Fully Homomorphic Encryption
MitM	Man-in-the-Middle
MGHE	Multi-Group Homomorphic Encryption
PIOP	Polynomial Interaction Oracle Proofs

IEEE	Institute of Electrical Electronics Engineering
ACM	Association of Computing Machinery
MLaaS	Machine Learning as a Service
CKKSS	Clean –Kim-Kim-Song Scheme
WAB-CPRE	Weighted Attribute-based Conditional Proxy Re-Encryption
LBPQC	Lattice-based Post-quantum Cryptography
IoT	Internet of Things
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analysis

SECTION II

Research Objectives

The objective of this research is to conduct a Systematic Literature Review (SLR) of homomorphic encryption schemes with focus on parties, platform, technique, computational complexities and limitations.

SECTION III

Structure of the Review

The structure of the review is presented section by section, showing the purpose of each part and providing a concise summary of the review. Section I introduces homomorphic encryption (HE), outlining its history, core concepts as well as explaining the privacy challenges and what motivate this systematic review. Section II discussed the aims of the review, mapping the research questions (RQs): RQ1 identifies the parties involved in HE systems, RQ2 describes platforms, RQ3 presents design techniques, RQ4 examines computational complexities, and RQ5 discusses limitations. Section III provides a summarizing roadmap that describes the contents of each major part to help readers navigate the review. Section IV critically perform survey of related literature, summarizing the scope and limitations of prior reviews. Section V describes the PRISMA-based methodology, including databases searched, search strings and keywords, date range, inclusion and exclusion criteria, the screening and selection workflow, and the data-extraction used in the systematic review. Section VI

presents the results and discussion, documenting records identified, screened, and included (with database breakdown) and key findings organized by RQ1–RQ5. Section VII outlines research directions and future work. Finally, the Conclusion summarizes the review's scope and the principal findings regarding HE.

SECTION IV

RELATED WORKS

Agbo et al. (2024a) conducted 21 primary studies surveys between 2013 - 2023. The research focus on various software applications specifically for student learning, curriculum development, delivery services, and more importantly for conducting student's assessment. The research work shows wider range of software solutions ranging from assessment tool to teaching applications with a distinct feature that supports learning which integrate lecture plan, lecture delivery, direct learning and management evaluation as the key benefit. The survey also highlights the challenges such cost of deployment, user self-interaction, efficacy and nervousness of software are the common factors that affects the complete adoption of this technological platforms at both the primary and secondary levels of education. Alloghani et al., (2019) uses the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) to analyze studies collected from different sources. Based on the literatures that was reviewed, it is certain that the security in big data and that of cloud computing received a greater percentage of interest by researchers. Several articles suggested the usage of HE nonetheless, thematic analysis has shown different worries with 38% of the article failed three checklist items. Result obtains through PRISMA and Cochrane Risk of Bias Tool shows that most of the research articles focused on the potentials use and the implementation of HE as a solution to the growing demands of big data and lack of security and privacy within. Behera and Prathuri (2020) proposed method where data that inputted data should be encrypted first using HE. Machine learning algorithm such as linear regression could be applied on data that is encrypted first for prediction while at the same time preserving privacy and confidentiality of the data. The algorithm output is presented in ciphertext form and will require decryption process to view the plaintext. Edge computing on the other hand sought to address the constraint of cloud computing in a supporting situation and delay in sensitive service of the Internet of Things (IoT) time. It leverages on utilizing power of local computing close to the gadgets which serve as edges servers for timely and efficient services. However, edge computing faces challenges on how to distribute and oversee storing of information,

how to edge computing synergize with cloud computing for scalable services and safeguarding of security of the framework. The HE is a unique encryption scheme that permits computations of data to be performed on encrypted data directly without any need to decrypt the data. The main idea of HE is for expert to be able to apply the knowledge of mathematics and its operations such as the addition and multiplication or any type of an arbitrary function to be carried out on encrypted data (Adablanu *et al.*, 2024). A critical need to address integrity and security in HE system, particularly when applied in multi-party scenarios such as Multi Group Homomorphic Encryption (MGHE). The authors then proposed a proof system based on Polynomial Interaction Oracle Proofs (PIOPS) to ensure that public keys are well formed, and ciphertexts which is significant securing data against malicious adversaries (Hwang *et al.*, 2024). HE enables data sharing for operation without compromising its privacy. Direct mathematical operations are being carried out in HE on data that is encrypted and does not require any decryption. When an operation is executed, result is directly returned in its encrypted format ensuring that only the recipient of the data can see the results by decrypting it. The confidentiality of the data is highly maintained in HE even when the operations or computations performed on the data in an untrusted environment (Mohan Das Viswam, 2022). HE based vulnerability evaluation framework, where encrypted vulnerability data could be processed by a centralized server without decryption. Their results confirmed strong confidentiality—since data remained encrypted during computation—and moderate computational performance improvements compared to existing HE approaches. Nevertheless, the methodology assumed a single trusted aggregation node and utilized static key management, which limited resilience against active MitM attacks(Bao *et al.,* 2024). Furthermore, there HE implementation lacked dynamic integrity verification or threshold adaptability, meaning that once the aggregator's key or communication channel was compromised, the system had no self-correcting mechanism to detect or mitigate the manipulation of vulnerability scores in transit (Bao *et al.*, 2024). Wu et al., (2025b) work discusses the effectiveness and accuracy on the encrypted data computations as it is applied in Privacy-Preserving Machine Learning (PPML). A review on HE technologies was conducted with the primary aim to take advantage of the Cheon Kim-Kim-Song (CKKS) algorithm which supports the computations that has to do with floating point in mathematics. Additionally, recent review that focuses on the development of the following machine learning algorithms: K-Nearest Neighbor (KNN), K-means clustering algorithms and also face recognition integration with HE was carried out. In addition, the research focuses on the systematic exploration by integrating HE and Machine Learning (ML) from the fundamental technology implementation and maintain trade-off in

the performance of the algorithms. Shah and Sivakumar (2026b) research carryout a comparison based on different HE models with the aim of evaluating their qualitative and quantitative profits and impediments particularly in terms of ciphertext performance during the computation process. The study leverage on the artical bias of AI by enhancing privacy, secrecy and security. The practicability of HE real world application was also discussed. HE information is linked on its capability to improve privacy-preserving AI and the ability to maintain its computation possibility. Filaly et al., (2025) caried out deep analysis on symmetric, asymmetric and hybrid encryption techniques that was applied in Hadoop techniques used to preserve large number of datasets. New improvement such as blockchain and post quantum encryption has so far been applied to improve Hadoop security mechanism. A hybrid system of encryption is provided which is aimed at securing efficient data processing within Hadoop environment.

SECTION V

METHODOLOGY

In this section the authors outline the systematic approach employed to identify, screen articles, and review relevant literatures for Homomorphic Encryption techniques in data privacy. A structured framework, based on the Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) guidelines was used (Agbo et al., 2024). The reason for the choice of PRISMA was because of its flexibility and concise format of reporting scientific research of this kind and its ability to present an unbiased review process. from primary research efforts are gathered for investigation reviews on systematic literature reviews on Homomorphic Encryption Scheme used by parties, platforms, techniques, complexities and limitations(Agbo et al., 2024). Several rules used to conduct SLRs have been shown in several literature to collect evidences from differences sources In light of the above, the guideline for conducting SLRs mostly used are in the area of planning, then followed by conducting the research and lastly reporting align with this research.

A). Literature Search, Selection, and Review Framework

Figure 1 shows the systematic search and selection process for the SLR using five research databases namely; Science Direct, IEEE Xplore, ACM, Springer Link and Web of Science. The process is categorized into three main stages- Identification, Filtering and Inclusion based on five (5) adopted RQs (RQ1-RQ5). At the identification stage, a total of 21,205 studies were identified cut across the 5

research questions where RQ5 has the highest result 11,354, followed by RQ3 with 5217 studies, RQ2 and RQ4 recorded 2309 and 2263 studies respectively and RQ1 has the least with 63 records. During filtering, the identified studies were screened down to 549 records. Yet again RQ5 recorded highest with 307, while RQ2 recorded 93 and RQ3 showed 87. RQ4 was reduced to 45 records and RQ1 to 17. During the Inclusion phase, which is the final stage, the studies were evaluated strictly for inclusion in the study. RQ5 has the most final count with 16 papers, RQ3 and RQ2 resulted to 8 and 7 respectively and RQ1 recorded 0 inclusion, meaning there was none of the identified studies for that specific question which met the final criteria.

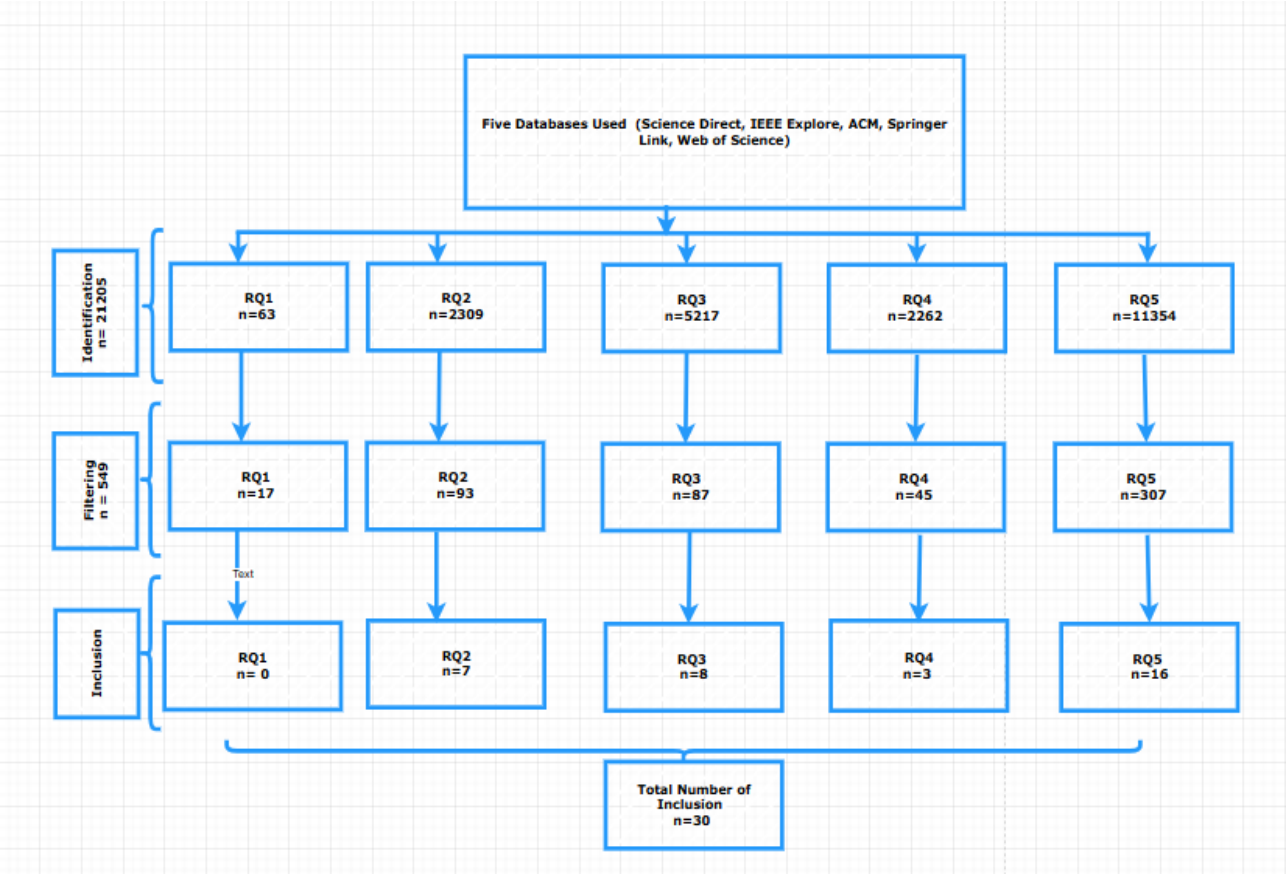

Figure 1 Study Selection Flowchart

A. Review Plan

The planning phase is the beginning. At the step the researcher recognized the necessity to conduct a SLR where we examine current software parties, platform, techniques and complexities used Homomorphic Encryption Scheme. This involved searching for existing, develop review and

implement collaborative discussions and reaching to adopt research questions, search, strategies and data collection processes and procedures.

1) Research Questions

Table 2 shows the formulation of the research question which are important for clarifying the main objectives of these research: exploring an existing information on homomorphic encryption scheme. After due consultation with the team that constitute this research, the following research questions will be considered.

Table 2: Research questions

SN	Question	Justification
RQ1	What are the parties involved in Homographic Encryption Schemes?	This clarify data owners, users, and cloud service providers roles and functions which is important for understanding the security implication, design effectiveness and compliance with policy in the domain of Homomorphic Encryption.
RQ2	What are the platforms used or deployed for the implementations of the Homomorphic Encryption?	This shows the tools and the environment that promotes homomorphic encryption in real time, thereby allowing a better understanding of their scalability and usability in real world scenarios application.
RQ3	What are the techniques used for the design, development and implementation of Homomorphic Encryption?	Various approaches and methodologies are explored in the execution of homomorphic encryption domain which is vital in assessing their effectiveness, security and safeguarding data while operation is allowed.
RQ4	What are the complexities in the design, development and practical or real-life implementation or deployment of Homomorphic Encryption?	This promote investigation of the numerous challenges and complications faced in creation of homomorphic encryption system, which is important in knowing their feasibility and potentials limitations in real time applications.
RQ5	What are the limitations of Homomorphic Encryption?	Several challenges and setbacks associated with homomorphic encryption techniques which is important for assessing it practicability and sets back in real time applications.

2) Sources of primary studies

A wider range of relevant publications for this study was explored by combining five well-known databases associated with the cybersecurity domain were used during initial search for the research. These databases include ScienceDirect, IEEE Xplore, ACM, SpringerLink and Web of science.

3) Defining the search research questions

In defining research question, it is important in the search process specifically include an output such as title and key terms that may be found in the body of each article reviewed. The research questions are as follows:

i. **Parties:** What are the parties involved in Homographic Encryption Schemes?
ii. **Platform:** What are the platforms used or deployed for the implementations of the Homomorphic Encryption?
iii. **Techniques:** What are the techniques used for the design, development and implementation of Homomorphic Encryption?
iv. **Complexities:** What are the complexities in the design, development and practical or real-life implementation or deployment of Homomorphic Encryption?
v. **Limitations:** What are the limitations of Homomorphic Encryption?

For example, if advance search feature is used in each of the data-based selected earlier, the research team specify the research question such as “What are the parties involved in Homographic Encryption Schemes” and so on to spot out articles that has germane titles may satisfy any key words given by the question in the body of the various articles.

4*) Inclusion and exclusion criteria used in the study*

Table 3 shows the detail inclusion criteria and also how the articles were excluded criteria**.** Upon getting the result from the first search for HE, the articles that appear are selected by applying the rules for the inclusion and exclusion standards. This procedure mainly identifies research work that may be relevant within the area of coverage of the SLR. This research attention is to classify current homomorphic encryption scheme in terms of parties, platform, technique and limitation; therefore, we review studies published over a period of five years (2020 - 2025) for several reasons. Articles must cover areas within computer science, cloud computing, and data security, highlighting relevant topics

such as multi-party, security, implementation and privacy. Excluded criteria consist of any publications related to blockchain, addressing attacks on HE, and non-research formats such as review articles, mini-reviews, surveys and conference papers. The criteria clearly emphasized that only open access articles should be considered, promoting wider accessibility to the research. In addition, publications focusing on techniques such as fully homomorphic encryption and federated learning challenges are required for inclusion. This systematic approach intends to curate a high-quality dataset that emphasizes significant advancements while filtering out less relevant or outdated studies.

Table 3: Inclusion and exclusion criteria

Research Questions	Identification	Filtering (Exclusion)	Inclusion
RQ 1	What are the parties involved in Homographic Encryption Schemes?	**Excluded Areas:** Review Articles, Book Chapters, Mini Reviews, Proceeding Books, Blockchain Content **Subject Area:** Research Articles **Access:** Open access **Date Range:** 2020-2025 **Focus:** Research Articles	Exploring HE for Security in Cloud, Fog, and Edge Computing, with a Focus on Federated Learning, Cryptography, and Multi-Party Security.
RQ 2	What are the platforms used or deployed for the implementations of the Homomorphic Encryption?	**Excluded Areas:** Attacks, Blockchain Content, Proceeding Books, Review Articles, Book Chapters, Mini Reviews **Subject Area:** Computer Science, Materials and Continua, Computer Security, Cybersecurity Applications **Access:** Open Access **Date Range:** 2020-2025 **Focus:** Research Articles	Implementation privacy homomorphism, Encrypted key-value systems, HE for MLaa by CKKS and Ciphertext retrieval, cloud and Fog computing, cloud computing with load balancing, Re-Encryption in the cloud
RQ 3	What are the techniques used for the design, development and implementation of Homomorphic Encryption?	**Excluded Areas:** Attacks and Blockchain **Subject Area:** Computer Science, Security, Cloud Computing, Data and Information Security **Access:** Open Access & Open Archives **Date Range:** 2020-2025 **Books:** Conferences, Proceeding Books excluded. **Focus:** Research Articles	Implementation privacy homomorphism, authentication scheme, FHE approach, homomorphic encryption,
RQ 4	What are the complexities in the design, development and practical or real-life implementation or deployment of Homomorphic Encryption?	**Excluded Areas:** Attacks, Blockchain, Proceeding Books, Review Articles, Book Chapters, Mini Reviews, Conferences **Subject Area:** Computer Science, Materials and Continua, Computer Security, Cybersecurity Applications, Cloud Computing, Data and Information Security **Access:** Open Access & Open Archives **Date Range:** 2020-2025 **Focus:** Research Articles	Integrity verification, preserving data privacy, Fully homomorphic encryption technique, privacy preservation,

RQ 5	What are the limitations of Homomorphic Encryption?	**Excluded Areas:** Attacks, Blockchain, Proceeding Books, Review Articles, Book Chapters, Mini Reviews, Conferences **Subject Area:** Computer Science, Computing Security, Cloud Computing, Data and Information Security, Materials and Continua, Cybersecurity Applications **Access:** Open Access & Open Archives **Date Range:** 2020-2025 **Focus:** Research Articles	Fully homomorphic encryption technique, privacy preservation, federated learning challenges, attack against federated learning,

B. Conducting the Review

In the second phase of conducting the SLR, the first step is to select five databases(Agbo *et al.*, 2024c) namely (ScienceDirect, IEEE Xplore, ACM, SpringerLink and Web of Science) to classify the studies that are pertinent to homomorphic encryption schemes used as a party, platform, complexities, techniques and limitations. In step 2, we entered the research questions on each search tab of the databases and collected results of each search which produced the total of identification $N_i = 21,205$ as shown in Table 3. After this, we conducted filtering the results of the identified number to base on the exclusion parameters identified in Table 2 which produced number of filtered articles $N_f = 549$. In step 3 we selected the research article by using exclusion and inclusion parameters as shown in Table 2. The parameters for inclusion were applied to identify researches that are identified under the scope of the study. Conversely the parameters for the exclusion were clearly applied to remove articles that are not identified under the scope of the study and eventually have not met the basic requirement for evaluating the articles, hence a total number of included articles to N= 43. We identify these as the Scopus index articles what has adequate information that fits the scope of the research based on questions set at the beginning of the research. During the fourth step, the author removed related data that are required and then record them on a excel spreadsheets for data analysis and report generation.

C. Reporting Review

The report and review process focuses on research findings from the selected studies. Thereafter, the implication of the findings were discussed based on the research questions RQ1, RQ2, RQ3, RQ4 and RQ5. This aim to response to the research questions outlined during the planning state. This information provide a comprehensive review on Homomorphic Encryption Schemes.

SECTION SIX

RESULTS AND DISCUSSION

The systematic review and meta-analysis of the selected studies on homomorphic encryption schemes. parties, platforms, techniques, complexities and limitations reveal the potential benefits, the inherent challenges and the open issues of these schemes.

After detailed screening of the identified Scopus index article, we then obtained a final number of selected studies to 40 which were critically analyzed based as shown on table 4.

Table 4.1: ***Statistics of The Research Article by Database for Homomorphic Encryption Study***.

Table 4.1 show the searches conducted in five difference research databases namely Science direct, IEEE Explore, ACM, Springer Link and Web of science. The number of entries retrieve during the identification stage is 21,205. Initial identification was conducted on the five (5) Research Questions (RQ), (RQ1-RQ5) across the five databases and returned RQ1=89 entries, RQ2=2409 entries, RQ3=5312 entries, RQ4 = 2310 entries and RQ5 = 11,677 entries. At the screening, 549 records were filtered out and 43 entries were at first identified for inclusion while 3 duplicates entries were also identified and removed, leaving 40 identified and included for all the studies. Additionally, based on the RQ the final inclusions were RQ1=0 included, RQ2=7 included, RQ3= 8 included, RQ4=3 included and RQ5= 16 were included. Finally, Science Direct recorded the largest number of hits for most questions, while IEEE Explore and Web of Science recorded the second largest hits; ACM and Springer Link recorded a substantial number for some RQs.

Table 4 Statistical Research Articles by different Databases

Activity	Science Direct	IEEE Explore	ACM	Springer Link	Web of Science	Total
RQ 1: Question						
Activity	**Science Direct**	**IEEE Explore**	**ACM**	**Springer Link**	**Web of Science**	**Total**
Identification	29	2	26	9	6	63
Filtering	10	1	2	4	0	17
Inclusion	0	0	0	0	0	0
Total	39	3	28	13	6	89
RQ 2: Question						
Activity	**Science Direct**	**IEEE Explore**	**ACM**	**Springer Link**	**Web of Science**	**Total**
Identification	1744	5	93	292	175	2309
Filtering	55	0	30	4	4	93
Inclusion	6	0	0	1	0	7
Total	1805	5	123	297	179	2409
RQ 3: Question						
Activity	**Science Direct**	**IEEE Explore**	**ACM**	**Springer Link**	**Web of Science**	**Total**
Identification	2459	10	329	1358	1061	5217
Filtering	14	0	3	42	28	87
Inclusion	2	0	2	4	0	8
Total	2475	10	334	1404	1089	5312
RQ 4: Question						
Activity	**Science Direct**	**IEEE Explore**	**ACM**	**Springer Link**	**Web of Science**	**Total**
Identification	810	0	10	127	1315	2262
Filtering	6	0	1	9	29	45
Inclusion	3	0	0	0	0	3
Total	819	0	11	136	1344	2310
RQ 5: Question						
Activity	**Science Direct**	**IEEE Explore**	**ACM**	**Springer Link**	**Web of Science**	**Total**
Identification	3511	257	5241	2341	4	11354
Filtering	14	29	261	1	2	307
Inclusion	3	7	4	2	0	16
Total	3528	293	5506	2344	6	11677
Total No of Identification = 21,205		**Total No of Filtering = 549**		**Total No. of Inclusion with Duplicates = 34** **Duplicated identified =3** **Total No. of Inclusion without Duplicates = 30**		

A). Homomorphic Encryption Parties

Figure 2 shows that the graph represents primary studies for RQ 1 based on their databases with four different steps. First are the stages of selection, where the colors represent: blue as Identification, which represents the initial papers found in each database using the specified RQ 1; orange as Filtering, where the number of papers that remained after the initial screening represents the first significant reduction; and gray as Inclusion, where the final set of papers that passed the full assessment against the rigorous inclusion and exclusion criteria is shown.

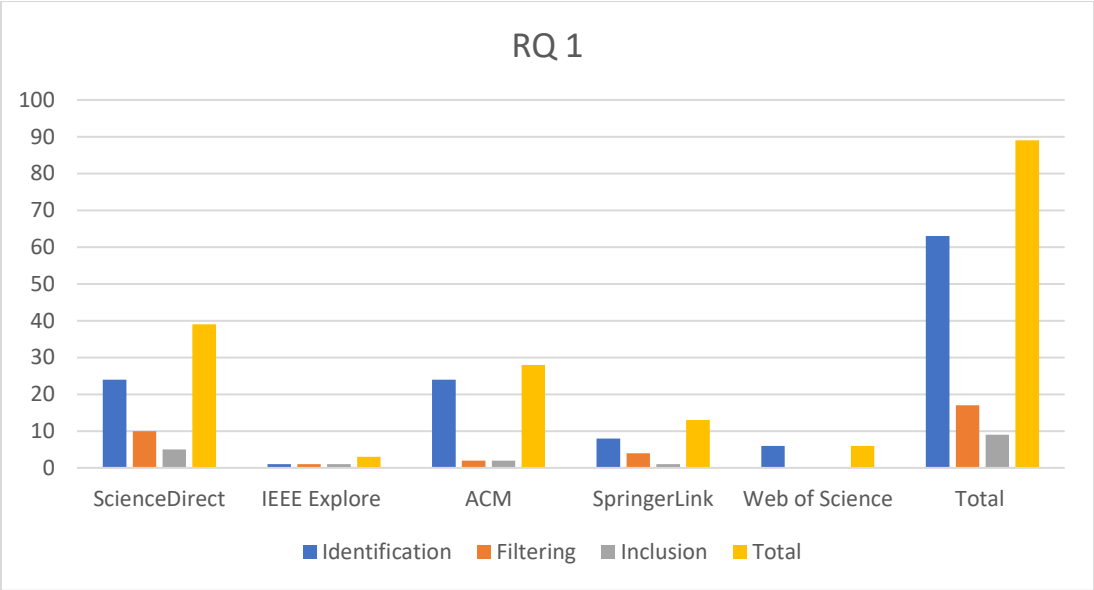

Figure 2. What are the parties involved in Homographic Encryption Schemes?

These 9 papers are primary studies that were used to answer RQ 1. Science Direct provided the highest number of final inclusion studies, having 4 out of 9, making it the most effective. ACM had a high rejection rate during filtering, contributing to 2 final articles. SpringerLink, Web of Science, and IEEE Xplore recorded none included paper for final full text review. The overall total column summarizes that the total identified were 63 found across five databases; after applying Filtering, which is the initial screening, the pool was reduced to 17 articles, and only 9 articles were finally selected for final review.

B). Homomorphic Encryption Platforms

Figure 3 represent the bar chart labelled RQ 2 which show the result of the SLR process for the second research question. The graph presents the studies found in different databases across the three-selection process Identification, filtering and inclusion.

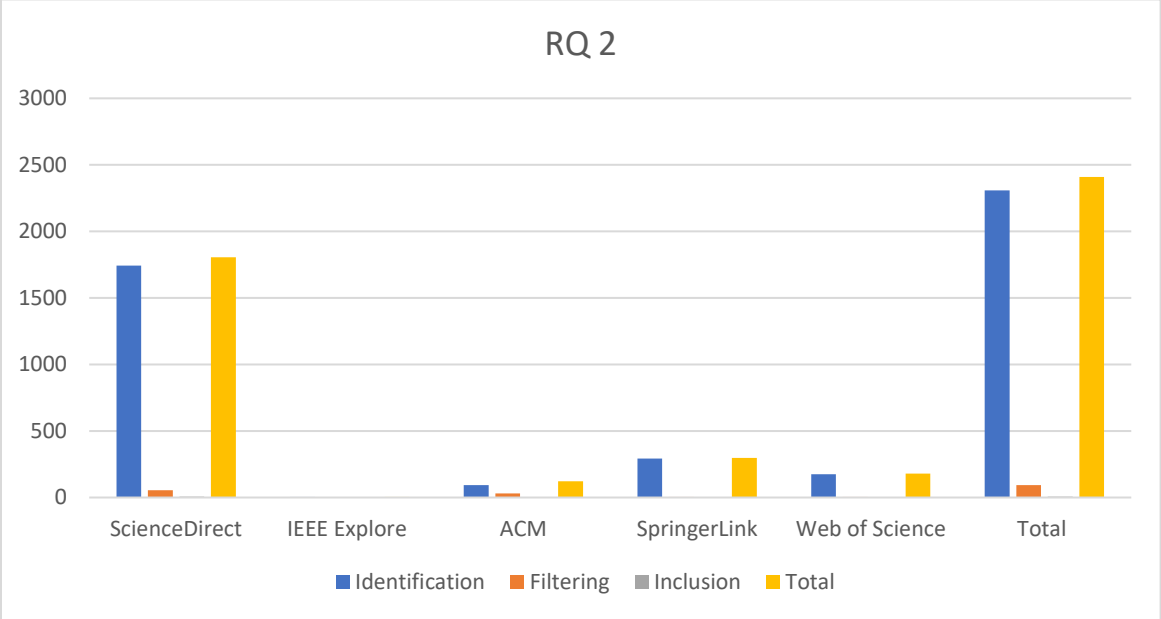

Figure 3. What are the platforms used or deployed for the implementations of the Homomorphic Encryption?

The identification in blue colour represents the initial detail of papers retrieved from each database based on the specified RQ 2 where raw result are pool. The filtering presented in orange colour represents the number of papers excluded, the inclusion presented in Grey colour represents the final set of papers that are successful which that passed the full assessment against the rigorous inclusion and exclusion criteria while the total presented in yellow appears to show the sum number of identified papers for each database identified. ScienceDirect shows one of highest number initially identified, 6 articles were included. IEEE Xplore returned no article for inclusion as well as ACM. SpringerLink and Web of Science contributed a moderate number of identified papers. Total identified is 2409 across the five databases. after applying Filtering, which is the initial screening, the pool was reduced to 93 articles, and only 7 articles were finally selected for final review.

Our findings on various platforms installed for the execution of homomorphic encryption: a study based on the implementation of homomorphic encryption is targeted at cloud storage environment,

utilizing cloud bases as platforms that supports secure processing and retrieval while ensuring data confidentiality and user privacy. DFHV-algorithm technique was used to enhance security and retrieval functionalities in these platforms (Hu *et al.*, 2025) . CKKS scheme was deployed on cloud computing platforms for Machine-Learning-as-a-Service (MLaaS). The RP-OKC framework is employed utilizing the library called TenSEAL which enable private-preserving data analytics during the entire period of efficient encrypted computations(Chang *et al.*, 2025). (Zhang *et al.*, 2025) implemented homomorphic encryption in federated learning algorithm that was proposed which utilizes a central server for gradient aggregation and distributed participants for local training. A secure computation framework with microservices architecture to manage privacy-preserving calculations in power big data environments was deployed. Hierarchical Privacy Protection Model in that is applied in advanced metering infrastructure that utilizes cloud and fog computing to implement homomorphic encryption for secure data processing was proposed by (Kuang and Zhang, 2024). The model combines smart meters, fogs nodes and cloud server to ensure effective data transmission and data privacy protection in a smart grid environment. An architecture for Hybrid Mobile Cloud computing was proposed that incorporates cloud and edge computing platforms for healthcare applications, using homomorphic encryption for data transmission security and processing. The proposed architecture enables load balancing to optimize latency and energy efficient while safeguarding patient privacy information (Lee *et al.*, 2023). A technique comprised of weighted-based Conditional Proxy Re-Encryption (WAB-CPRE) was designed and implemented in cloud environment, thereby allowing a secure data access control and sharing via cloud services. It leverages on a combination of cloud service providers and management of encrypted data which promote effective, efficient and flexible user access and sharing while privacy and security are maintained (Yan, Zhang and Cheng, 2025).

C). Homomorphic Encryption Techniques

The figure 4 represent the bar chart labelled RQ 3 which show the result of the SLR process for the second research question. The graph presents the studies found in different databases across the three-selection process Identification, filtering and inclusion.

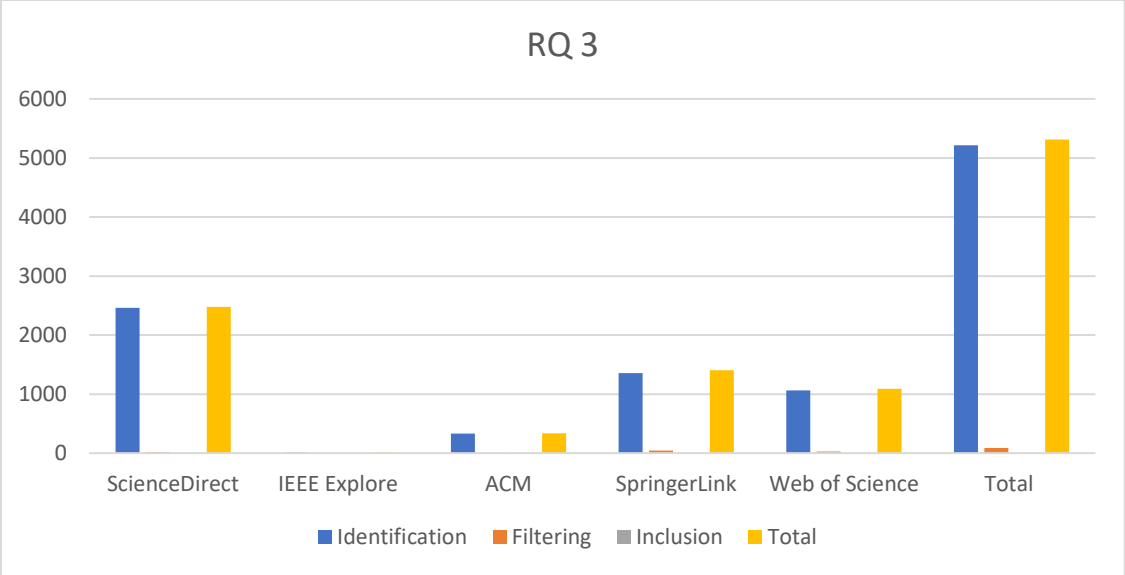

Figure 4 What are the techniques used for the design, development and implementation of Homomorphic Encryption?

The identification in blue colour represents the initial detail of papers retrieved from each database based on the specified RQ 3 where raw result are pool. The filtering presented in orange colour represents the number of papers excluded, the inclusion presented in Grey colour represents the final set of papers that are successful which that passed the full assessment against the rigorous inclusion and exclusion criteria while the total presented in yellow appears to show the sum number of identified papers for each database identified. ScienceDirect provided the highest number initially identified, 2 articles were at last included. IEEE Xplore and Web of Science recorded none articles for inclusion. SpringerLink and ACM recorded 4 and 2 respectively for inclusion. Total identified is 5312 across the five databases. after applying Filtering, which is the initial screening, the pool was reduced to 87 articles, and only 8 final reviewed articles were selected.

Findings from this research is on the techniques used for the design, development, and implementation of homomorphic encryption suggest that a framework was proposed for implementing homomorphism-based privacy. This framework utilizes encoding techniques and computations managed by a secure remote server, employing a single slope ADCs for data encoding. It generates look-up for efficient computations and uses SHA-3 for generating pseudorandom permutations to maintain data confidentiality(Hutto and Mooney, 2025). Hung et al. (2025) proposed a selective end to end data sharing framework which combine proxy re-encryption and redactable signature scheme

to achieve data confidentiality and authenticity while enabling nuanced selective disclosure. Modular cryptographic blocks and their implementation through various algorithms is developed and implemented via different algorithms ensuring a secure data management and adaptability in cloud environments. A biometric authentication scheme combines with Support Vector Machine (SVM) with Zero Knowledge Proof (ZKP) to ensure privacy protection without disclosing a template of biometric while addressing security vulnerability in existing systems. It ensures efficient enrollment and process of authentication that protect users' confidentiality using polynomial techniques(Guo *et al.*, 2024). The application of Fully Homomorphic Encryption (FHE) in a distributed clustering protocol for time series data, local differential privacy was combined to enhance privacy while maintaining data utilization. Techniques for implementation which include agent-based modeling, secure communication protocol and local caching strategies to optimize efficiency in computations and confidentiality guarantees(Álvarez and Menci, 2025a).Several techniques to enhance Homomorphic Encryption including secure outsourcing, execution of hardware-based trust and optimized representations for efficient computations on resources constrained devices and large-scale data. The need for adaptable solutions is stressed for real world-applications within the internet of things context (IOTs) and Big data(Gamiz *et al.*, 2025) A NeuroCrypt is developed, it is a hybrid technique that fully integrated FHE with LSTM-based anomaly detection and blockchain to secure IoTs network devices. It optimizes the implementation of ciphertext packing and model quantization achieving 99.2% of detection accuracy while data privacy and confidentiality s maintained in real time(Kumar *et al.*, 2025). A novel protocol which combines Paillier Homomorphic cryptosystems with Zero-Knowledge Proofs to enable privacy-based access control. It shows how multiple private attributes can be evaluated against policies concurrently without the system owner learning the actual values effectively while securing sensitive data(Kumar *et al.*, 2025) A framework that also combines Lattice Based Post-Quantum Cryptography (LBPQC) with homomorphic Encryption and blockchain to secure users' data in cloud surroundings. Third party are allowed to verify data integrity through ZKP without ever reading the original content achieving high accuracy and a significant reduction in privacy leakage (Khan *et al.*, 2025).

D. Homomorphic Encryption Complexities

Figure 5 represent the bar chart labelled RQ 4 which show the result of the SLR process for the second research question. The graph presents the studies found in different databases across the three-selection process Identification, filtering and inclusion.

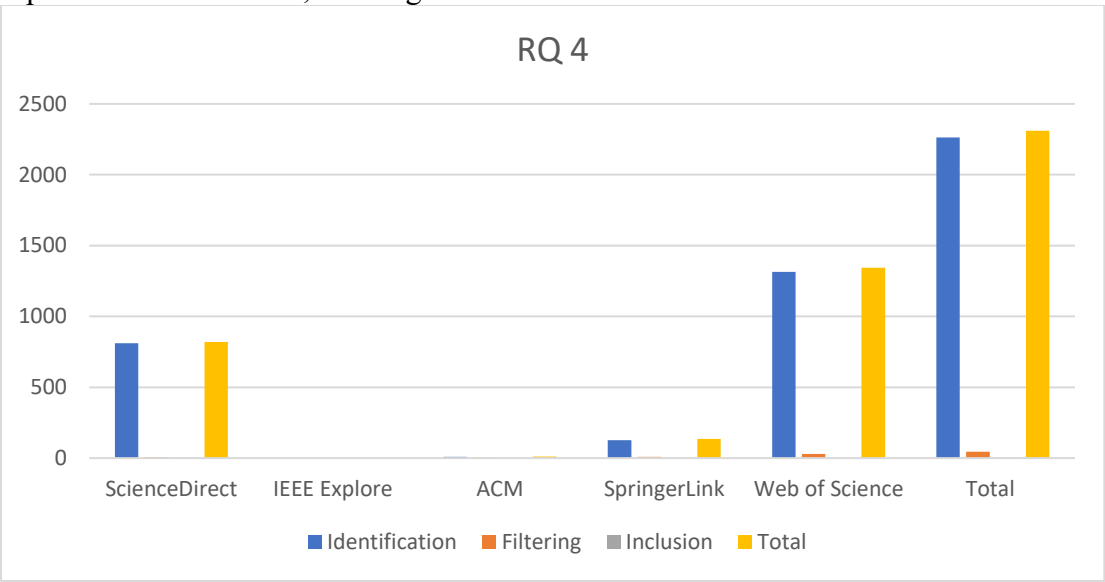

Figure 5. What are the complexities in the design, development and practical or real-life implementation or deployment of Homomorphic Encryption?

The identification in blue colour represents the initial detail of papers retrieved from each database based on the specified RQ 4 where raw result are pool. The filtering presented in orange colour represents the number of papers excluded, the inclusion presented in Grey colour represents the final set of papers that are successful which that passed the full assessment against the rigorous inclusion and exclusion criteria while the total presented in yellow appears to show the sum number of identified papers for each database identified. ScienceDirect recorded the second highest number initially identified with 3 articles included at last whereas Web of Science recorded the highest. IEEE Xplore, Web of Science, SpringerLink and ACM recorded none articles for inclusion. Total identified is 2310 across the five databases. After applying Filtering, which is the initial screening, the pool was reduced to 45 articles, and only 3 articles were finally selected for final review.

The complexities in the design, development and practical or real-life implementation of homomorphic encryption scheme is highlighted due to its massive computational overhead and the mathematical difficulty of performing non-linear operations on encrypted data. Additionally, practical deployment is prevented by lack of regulatory incentive for adoption and high resources demands by

edge computing which necessitates a complex architecture to maintain system efficiency (Liu and Biczók, 2025). Li et al. (2025) also highlight the complexities in the design and development of a secure data auditing and encryption scheme stem from massive computational and storage overheads required to manage data structures and a times metadata. The technical burdens combined with emerging threat of quantum computing usually result in system that find it difficult to scale through or applying it on a distributed network and cloud environments. Homomorphic Encryption designs are usually complicated by high computational cost and the necessity of using complex polynomial approximations for non-linear operations, thereby leading to accuracy reduction. Additionally, the accumulation of computational noise that requires resources intensive bootstrapping to manage is prevented by extreme latency and memory demands(El Mestari, Lenzini and Demirci, 2024a).

E). Homomorphic Encryption Limitations

Figure 6 represent the bar chart labelled RQ 4 which show the result of the SLR process for the second research question. The graph presents the studies found in different databases across the three-selection process Identification, filtering and inclusion.

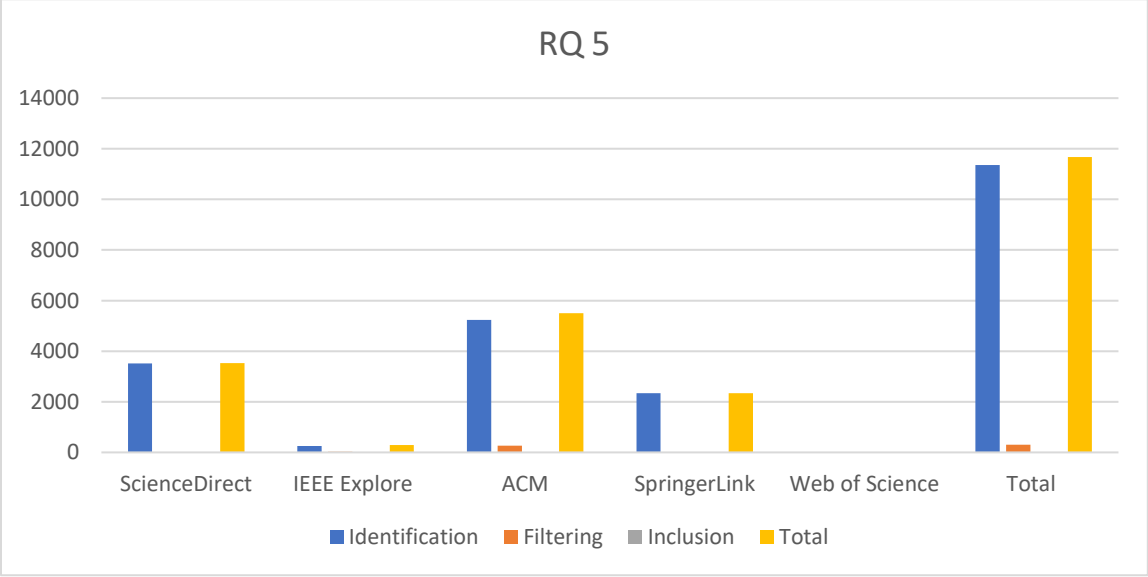

Figure 6. What are the limitations of Homomorphic Encryption?

The identification in blue colour represents the initial detail of papers retrieved from each database based on the specified RQ 4 where raw result are pool. The filtering presented in orange colour

represents the number of papers excluded, the inclusion presented in Grey colour represents the final set of papers that are successful which that passed the full assessment against the rigorous inclusion and exclusion criteria while the total presented in yellow appears to show the sum number of identified papers for each database identified. ACM recorded the highest number initially identified with 4 articles included, ScienceDirect recorded the second highest number initially identified with 3 articles for inclusion. IEEE Xplore and SpringerLink recorded 7 and 2 respectively for inclusion where Web of Science recorded none articles for inclusion. Total identified is 11677 across the five databases. After applying Filtering, which is the initial screening, the pool was reduced to 307 articles, and the final selected reviewed articles were only 16.

The findings indicate that limitations of homomorphic encryption scheme are related to the high computational cost for performing encryption and operations thereby reducing the system efficiency and performance that result from attempting to balance privacy trade-offs (Lewis, Varadharajan and Noman, 2023). Traditional homomorphic encryption scheme in federated learning is limited by its inability to defend against backdoors attacks, poisoning and deficiencies in reliance on shared keys or complex multi-party computations for decryption. Additionally, Homomorphic proxy re-encryption systems has issues with scalability due to high computations and communications costs of re-encrypting data for only one receiver(Fan *et al.*, 2022). HE is primarily limited by significant computational overhead and large cipher text sizes, which result in high processing latency and increased communication times compared to operations of plaintext. These limitations often need the use of lightweight models and high-performance hardware like GPUs to make real-time applications accessible (Cha *et al.*, 2025). HE in federated learning is seen with excessive computation and storage overhead and can cause data to expand thereby reducing the slow calculation speed. Also training with HE was estimated to take over 400 hours making it currently unacceptable for practical (Hu *et al.*, 2022). HE basically struggles with complex non-linear operations required by deep learning models, often requiring approximations that can reduce accuracy. This limitation, coupled with high computational costs and challenges in scaling to deeper architectures, restricts HE's applicability practically (Nguyen *et al.*, 2025). HE increases the size and complexity of transmitted data significantly; this poses challenges for bandwidth-limited edge computing devices and increases high communication overhead. It also introduces substantial computational overhead which increased latency, making real-time implementation difficult, especially in resource-constrained environments (Rahbari, Daneshtalab and Jenihhin, 2025).Xu et al. (2024) discusses the homomorphic operations

which include operations such as: addition, multiplication, scalar multiplication, rotation, encryption, and decryption, are extremely time-consuming, contributing significantly to computational overhead. A significant computational overhead was introduced due to homomorphic encryption and decryption operations, particularly for deep neural networks with numerous parameters. This essential complexity challenges the runtime and memory efficiency of systems utilizing HE, making HE a critical area for optimization in privacy-preserving applications(Li, Tan and Shin, 2025). HE significantly increases computational overhead, usually from operating 1,000 to 10,000 times slower than plaintext operations and incurring 100 to 1,000 times higher communication costs. In spite of these inadequacies, it offers a near-perfect privacy with negligible accuracy loss, making it suitable for privacy-critical applications where computational cost is secondary. Fully homomorphic encryption (FHE) is limited by its excessive computational complexity, making its practical application challenging despite its theoretical potential for privacy-preserving computations(Su *et al.*, 2020). HE schemes are limited by supporting basic arithmetic operations such as addition and multiplication, making them incompatible with mathematical functions such as rounding or non-polynomial evaluations. Additionally, the scheme suffers from high computational costs and increased computing time(Akram *et al.*, 2024). HE schemes are basically limited to basic arithmetic operations, making them incompatible with high-level and non-polynomial functions, which leads to loss in accuracy and noise through approximations in some instances. This limitation, which is associated with high computational costs and increased processing time required for complex operations in homomorphic and deeper computations, poses significant efficiency challenges(El Mestari and Demirci, 2024). HE schemes are primarily limited by only supporting basic arithmetic operations, which makes them unsuitable for complex non-linear functions which is essential in modern machine learning. Furthermore, existing HE methods suffer from significant computational overhead, rendering them impractical for large-scale, real-world machine learning(El Mestari, Lenzini and Demirci, 2024b). HE is associated with computationally expensive and intensive, which limits the use in practical applications. Additionally, certain mathematical operations like square roots pose specific technical limitations, leading researchers to use substitutes like squared Euclidean distance to maintain accuracy in encrypted domains(Álvarez, Fernández and Menci, 2025b). The comparative studies identify some of the best practices for deploying homomorphic encryption across platforms and application domain. These studies enlighten the research community on the professional training targeting various stakeholders such as software developers, administrators and information technology specialist. These categories of professionals

would enable them adapt to complexities of homomorphic encryption and its integration in existing technological domain. More so, investigating the strategies to overcome the bottlenecks such as low the complexities and cryptography self-efficacy around the overheads and usability remain a critical area of research. The impact of various mechanism for supports such as robust technical documentations, expert mentoring and application of these tool may be evaluated by researchers working on homomorphic encryption.

SECTION VII

Research Directions

Table 4.2 presents the summary of open research gabs. These gabs futured across two domains as impact were measured between educational and homomorphic encryption technologies.

Table 4.2 Research directions

S/N	Authors	Open issues	Research Direction
1	(Agbo et al., 2024)	The influence of current educational software on various students plus the special needs is not thoroughly examine	Research should concentrate on how to assess the long-term influence of educational software on student learning outcome, teacher efficiencies and class rooms' dynamics.
2	(Alloghani *et al.*, 2019)	The application of FHE will gain traction if research is relied on quantum computing	Development of post quantum resistance FHE with reduce key sizes and computational overhead to secure computations on big Data and cloud platforms
3	(Wu et al., 2025)	At present, the computational complexity of HE technology is quite high, which will have some restriction in its application especially when implementing on big datasets	The focus should be geared towards algorithm optimization and practical development to lessen the computational complexity and improve the effectiveness of encryption and decryption algorithms.
4	(Shah and Sivakumar, 2026)	The performance results from the study shows a disjointed results among all research articles. This makes it difficult to compare and conclude on the findings. The solution is to develop a framework that would be unified and would serve as a benchmark to	Priority should be given to the creation of standardized benchmarking protocols that would be used to evaluate encryption schemes in specifically for AI applications.

		assess all encryption methods across different workloads which would also including federated learning, and large-scale cloud-based analytics.	
5	(Filaly *et al.*, 2025)	A reasonable computing power is required when processing large encrypted datasets in distributed architecture such as the Hadoop. If not sufficient, might limit system scalability and can slow down operations in real-time. The complication of key management in large-scale systems is another key hindrance. Implementing an effective key sharing policy is vital for symmetric encryption, but becomes difficult to handle as the number of nodes in the Hadoop cluster increases.	The advice is to concentrate on perceptions of AI-controlled anomalies in with the aim of proactively detect and alleviate security threats using. The application of deep learning models that is trained on distributed data records without abusing user privacy is necessary.

SECTION VII

CONCLUSION

The systematic literature review (SLR) conducted in this study offers a detail assessment of the present state of homomorphic encryption (HE) Schemes between 2020 and 2026. By investigating 40 unique primary studies across five major databases, the research successfully mapped the landscape of HE through five critical lenses, participating parties, deployment platforms, design techniques, operational complexities, and inherent limitations.

The research identifies a various technique, including the integration of Zero-Knowledge Proofs and Federated Learning, yet these are consistently hindered by massive computational overhead and high latency. Our Findings disclose that operations can be up to 10,000 times slower than plaintext, hence, highlighting a critical need for optimization in handling non-linear functions and large ciphertext sizes. Ultimately, again the research study provides a clear understanding of current complexities, suggesting that future feasibility depends on balancing near-perfect privacy with improved resource efficiency. The SLR shows that while HE offers near-perfect privacy, it is currently burdened by massive computational overhead, large ciphertext sizes, and difficulty executing non-linear operations. These

complexities require specialized hardware like GPUs or the development of lightweight models for resource-constrained IoT environments.

AUTHOR CONTRIBUTIONS

J.E. Mamza Conceptualize the SLR, Methodology, Data correction, Results analysis, writing the report and also the original draft. He also carry out the review and the editing. **I. Ismaila:** Overall **s**upervision, part of the write-up and editing. He also validate and carry out analysis of the work. **J. A. Ojeniyi:** Supervision, review, and editing of the work. He also carryout data vitualization data correction and forensics investigation of the data used. **S.M. Abdulhamid**, Investigation, writing – review & editing, Visualization and formal analysis and **M.D. Noel:** Supervision, review writing and document editing. He also carry out data visualization and investigation. **S. Ahmad** Carry out investigation, script writing, review, document editing and formal analysis.

REFERENCES

‘Adablanu, S. *et al.* (2024) ‘Homomorphic Encryption for Secure Cloud Computing Homomorphic Encryption for Secure Cloud Computing Homomorphic Encryption for Secure Cloud Computing’. doi: 10.13140/RG.2.2.19574.41285.

Agbo, B. *et al.* (2024a) ‘A systematic literature review on software applications used to support curriculum development and delivery in primary and secondary education’, *International Journal of Educational Research Open*, 7. doi: 10.1016/j.ijedro.2024.100385.

Agbo, B. *et al.* (2024b) ‘A systematic literature review on software applications used to support curriculum development and delivery in primary and secondary education’, *International Journal of Educational Research Open*, 7. doi: 10.1016/j.ijedro.2024.100385.

Agbo, B. *et al.* (2024c) ‘A systematic literature review on software applications used to support curriculum development and delivery in primary and secondary education’, *International Journal of Educational Research Open*, 7. doi: 10.1016/j.ijedro.2024.100385.

Ahn, J. *et al.* (2025) ‘Exploring Encryption Algorithms and Network Protocols: A Comprehensive Survey of Threats and Vulnerabilities’, *IEEE Communications Surveys and Tutorials*. doi: 10.1109/COMST.2025.3526605.

Akram, A. *et al.* (2024) ‘Privacy Preserving Inference for Deep Neural Networks: Optimizing Homomorphic Encryption for Efficient and Secure Classification’, *IEEE Access*, 12, pp. 15684–15695. doi: 10.1109/ACCESS.2024.3357145.

Alloghani, M. *et al.* (2019) 'A systematic review on the status and progress of homomorphic encryption technologies', *Journal of Information Security and Applications*, 48. doi: 10.1016/j.jisa.2019.102362.

Álvarez, I. A., Fernández, J. D. and Menci, S. P. (2025a) 'Privacy-preserving distributed clustering: A fully homomorphic encrypted approach for time series', *Computers and Security*, 157. doi: 10.1016/j.cose.2025.104579.

Álvarez, I. A., Fernández, J. D. and Menci, S. P. (2025b) 'Privacy-preserving distributed clustering: A fully homomorphic encrypted approach for time series', *Computers and Security*, 157. doi: 10.1016/j.cose.2025.104579.

Bao, H. *et al.* (2024) 'Secure multiparty computation protocol based on homomorphic encryption and its application in blockchain', *Heliyon*, 10(14). doi: 10.1016/j.heliyon.2024.e34458.

Chang, R. I. *et al.* (2025) 'Approximate Homomorphic Encryption for MLaaS by CKKS with Operation-Error-Bound', *Computers, Materials and Continua*, 85(1), pp. 503–518. doi: 10.32604/cmc.2025.068516.

Fan, C. I. *et al.* (2022) 'ID-Based Multireceiver Homomorphic Proxy Re-Encryption in Federated Learning', *ACM Transactions on Sensor Networks*, 18(4). doi: 10.1145/3540199.

Filaly, Y. *et al.* (2025) 'A comprehensive survey on big data privacy and Hadoop security: Insights into encryption mechanisms and emerging trends', *Results in Engineering*. Elsevier B.V. doi: 10.1016/j.rineng.2025.106203.

Gamiz, I. *et al.* (2025) 'Challenges and future research directions in secure multi-party computation for resource-constrained devices and large-scale computations', *International Journal of Information Security*, 24(1). doi: 10.1007/s10207-024-00939-4.

Guo, C. *et al.* (2024) 'A novel biometric authentication scheme with privacy protection based on SVM and ZKP', *Computers and Security*, 144. doi: 10.1016/j.cose.2024.103995.

Hu, R. *et al.* (2025) 'A Fully Homomorphic Encryption Scheme Suitable for Ciphertext Retrieval', *Computers, Materials and Continua*, 84(1), pp. 937–956. doi: 10.32604/cmc.2025.062542.

Hu, S. *et al.* (2022) 'The OARF Benchmark Suite: Characterization and Implications for Federated Learning Systems', *ACM Transactions on Intelligent Systems and Technology*, 13(4). doi: 10.1145/3510540.

Hung, C. C. *et al.* (2025) 'ReLoaDing Performance: A Locality-Based Strategy for Rapid Reads in Encrypted Key-Value Systems', *ACM Transactions on Embedded Computing Systems*, 24(5 s). doi: 10.1145/3761810.

Hutto, K. and Mooney, V. (2025) 'Implementing Privacy Homomorphism with Random Encoding and Computation Controlled by a Remote Secure Server', *ACM Transactions on Embedded Computing Systems*, 24(2). doi: 10.1145/3651617.

Hwang, I. *et al.* (2024) *Practical Zero-Knowledge PIOP for Public Key and Ciphertext Generation in (Multi-Group) Homomorphic Encryption*.

Khan, A. A. *et al.* (2025) 'Quantum computing empowering blockchain technology with post quantum resistant cryptography for multimedia data privacy preservation in cloud-enabled public auditing platforms', *Journal of Cloud Computing*, 14(1). doi: 10.1186/s13677-025-00771-8.

Kuang, L., Shi, W. and Zhang, J. (2024) 'Hierarchical Privacy Protection Model in Advanced Metering Infrastructure Based on Cloud and Fog Assistance', *Computers, Materials and Continua*, 80(2), pp. 3193–3219. doi: 10.32604/cmc.2024.054377.

Kumar, S. *et al.* (2025) 'LSTM guided homomorphic encryption for threat-resistant IoT networks', *Discover Computing*, 28(1). doi: 10.1007/s10791-025-09843-4.

Lee, A. *et al.* (2023) 'Hybrid Mobile Cloud Computing Architecture with Load Balancing for Healthcare Systems', *Computers, Materials and Continua*, 74(1), pp. 435–452. doi: 10.32604/cmc.2023.029340.

Lewis, C., Varadharajan, V. and Noman, N. (2023) *Attacks against Federated Learning Defense Systems and their Mitigation*, *Journal of Machine Learning Research*. Available at: http://jmlr.org/papers/v24/22-0014.html.

Li, F. *et al.* (2025) 'Integrity verification scheme for distributed dynamic data in service ecosystems', *Computers and Security*, 159. doi: 10.1016/j.cose.2025.104671.

Li, Y., Tan, Q. and Shin, B. S. (2025) 'CryptoGAN: Privacy-Preserving Federated Generative Adversarial Networks With Homomorphic Encryption in Healthcare Systems', *IEEE Transactions on Computational Social Systems*. doi: 10.1109/TCSS.2025.3570990.

Liu, S. and Biczók, G. (2025) 'IDPFilter: Mitigating interdependent privacy issues in third-party apps', *Computers and Security*, 151. doi: 10.1016/j.cose.2025.104321.

El Mestari, S. Z., Lenzini, G. and Demirci, H. (2024a) 'Preserving data privacy in machine learning systems', *Computers and Security*, 137. doi: 10.1016/j.cose.2023.103605.

El Mestari, S. Z., Lenzini, G. and Demirci, H. (2024b) 'Preserving data privacy in machine learning systems', *Computers and Security*, 137. doi: 10.1016/j.cose.2023.103605.

Mohan Das Viswam (2022) 'a312b034_36_37_tup_homomorphic_encryption_compressed'.

Nguyen, L. *et al.* (2025) 'A Novel Polynomial Activation for Audio Classification Using Homomorphic Encryption', *IEEE Access*, 13, pp. 87834–87847. doi: 10.1109/ACCESS.2025.3571016.

Petticrew, M. and Roberts, H. (2006) *Systematic Reviews in the Social Sciences A PRACTICAL GUIDE*.

Rahbari, D., Daneshtalab, M. and Jenihhin, M. (2025) 'An Efficient Architecture for Edge AI Federated Learning With Homomorphic Encryption', *IEEE Access*, 13, pp. 97919–97929. doi: 10.1109/ACCESS.2025.3576689.

Behera, S and Prathuri, J.R (2020) ‘Application of Homomorphic Encryption in Machine Learning," 2020 2nd PhD Colloquium on Ethically Driven Innovation and Technology for Society (PhD EDITS), Bangalore, India, 2020, pp. 1-2, doi: 10.1109/PhDEDITS51180.2020.9315305’, *IEEE*.

Shah, A., Sivakumar, S. and N, P. (2026a) ‘Encrypted intelligence: A comparative analysis of homomorphic encryption frameworks for privacy-preserving AI’, *Journal of Economy and Technology*, 4, pp. 252–265. doi: 10.1016/j.ject.2025.08.001.

Shah, A., Sivakumar, S. and N, P. (2026b) ‘Encrypted intelligence: A comparative analysis of homomorphic encryption frameworks for privacy-preserving AI’, *Journal of Economy and Technology*, 4, pp. 252–265. doi: 10.1016/j.ject.2025.08.001.

Su, Y. *et al.* (2020) ‘FPGA-based hardware accelerator for leveled RIng-LWE fully homomorphic encryption’, *IEEE Access*, 8, pp. 168008–168025. doi: 10.1109/ACCESS.2020.3023255.

Wu, L. *et al.* (2025a) ‘Homomorphic Encryption for Machine Learning Applications with CKKS Algorithms: A Survey of Developments and Applications’, *Computers, Materials and Continua*. Tech Science Press, pp. 89–119. doi: 10.32604/cmc.2025.064346.

Wu, L. *et al.* (2025b) ‘Homomorphic Encryption for Machine Learning Applications with CKKS Algorithms: A Survey of Developments and Applications’, *Computers, Materials and Continua*. Tech Science Press, pp. 89–119. doi: 10.32604/cmc.2025.064346.

Xu, L. *et al.* (2024) ‘Cloud-Assisted Privacy-Preserving Spectral Clustering Algorithm Within a Multi-User Setting’, *IEEE Access*, 12, pp. 75965–75982. doi: 10.1109/ACCESS.2024.3404265.

Yan, X., Zhang, J. and Cheng, P. (2025) ‘Weighted Attribute Based Conditional Proxy Re-Encryption in the Cloud’, *Computers, Materials and Continua*, 83(1), pp. 1399–1414. doi: 10.32604/cmc.2025.059969.

Yousuf, H. *et al.* (2021) ‘Systematic Review on Fully Homomorphic Encryption Scheme and Its Application’, in *Studies in Systems, Decision and Control*. Springer, pp. 537–551. doi: 10.1007/978-3-030-47411-9_29.

Zhang, W. *et al.* (2025) ‘Design of a federated learning algorithm for power big data privacy computing based on pruning technique and homomorphic encryption’, *Egyptian Informatics Journal*, 32. doi: 10.1016/j.eij.2025.100828.